

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information Associated with
KREAMPIEQWERTY6@GMAIL.COM, Google Account
That Is Stored at Premises Controlled by Google, LLC

Case No. 1:24mj23

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
§ 2252A(a)(2)	Distribution of Child Pornography

The application is based on these facts:

See Attached Affidavit of Task Force Officer William M. Hargrove

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

On this day, the applicant appeared before me by reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

/s/ William M. Hargrove

Applicant's signature

William M. Hargrove, Task Force Officer, HSI

Printed name and title

Date: 01/18/24

City and state: Greensboro, North Carolina



Judge's signature

United States Magistrate Judge L. Patrick Auld

Printed name and title

ATTACHMENT A
(Property to be Searched)

“Notwithstanding Title 18, United States Code, Section 2252A, Google shall disclose responsive data, if any, by delivering encrypted files through Google's Law Enforcement Request System.”

This warrant applies to information associated with **kreampieqwerty6@gmail.com**, that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B
(Items to be Searched and Seized)

I. Information to be disclosed by Target providers.

To the extent that the information described in Attachment A is within the possession, custody, or control of the “Target Provider” (Google), the Target Provider is required to disclose the following information to the government for the accounts or identifiers listed in Attachment A (the “TARGET ACCOUNT”) **from August 1, 2022 to present**. Such information should include the below-described content of the subject accounts:

A. Location Data: Any location data currently stored in relation to the TARGET ACCOUNT or associated device(s). This includes any historical physical addresses, latitude and longitude data, estimated latitude and longitude location data, location history, or any other data captured and stored by Google by the listed Gmail user that would aid law enforcement in establishing historical location information related to the Gmail account use.

1. To include any historical location data, whether it be in the form of GPS, Wi-Fi, Cellular or Bluetooth readings collected by device, regardless if contained within the TARGET ACCOUNT or associated device(s) location history settings.
2. To include any Wi-Fi Access Points, SSID’s and MAC addresses in which the device has connected to for the aforementioned period.
3. This would further include all information stored and maintained in the “My Activity” associated with the TARGET ACCOUNT. Specifically, all

information currently stored in reference to the users "Timeline in Google Maps;"

- B. Location History** for any device that has logged into the TARGET ACCOUNT, for the aforementioned requested time period. Location information can be in the form of historical records and semantic location history records. Specific to Google, this would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information;
- C. Account Information:** To include all account owner/user identification information, to include all information listed in the "your personal info" within the Google My Account screen. This is to include any stored data that would aid in identifying the user/owner of the TARGET ACCOUNT. Any IP addresses related data access, logins, or browsing history, forwarding phone numbers, SMS forwarding numbers, alternate email addresses, and any linked social media accounts would be included in this request. Further included in "account information" is all information currently stored in reference to the users account to include, Google search history, websites visited history, map search history, and any other information associated with location history, device information and recently used devices;
- D. Google Accounts linked by Cookies:** In the event any identified Account information is connected to other Google Accounts by internet cookies, please

provide any and all data identifying date/time of Account creation and Internet Protocol utilized;

- E. **Internet Protocol version 6 (IPv6) and version 4 (IPv4):** Any data currently stored in relation to the email address or devices accessing email address identified below or associated with the TARGET ACCOUNT. To include all Internet Protocol address (IPV4 with source port and IPV6, if available) logs for user communication/email activity that would aid law enforcement in establishing historical location information related to the TARGET ACCOUNT use;
- F. **Application History:** To include all apps downloaded from the Google Play Store to the current devices associated with the TARGET ACCOUNT or associated device(s). This request will include the association of each app to a specific device when available and the date the app was downloaded;
- G. **Browsing and Search History:** To include all browsing history. This history includes the list of web pages a user has visited recently, as well as associated data such as page title and time of visit. To include all search history. This history includes the searched for terms, the date and time of the search, and the user selected results, including the specific terms searched in association with the TARGET ACCOUNT, the dates, times and time zones of all searches, the IP addresses or telephone or instrument identifying numbers associated with those searches, and any data related to the results of the searches

associated with the TARGET ACCOUNT and the TARGET ACCOUNTS' use of any search results;

- H. **Email Content:** Any Email Content currently stored in relation to the TARGET ACCOUNT. To include Non-Content information, originating message IP Addresses, Account Settings, email content to include deleted emails. The contents of all emails stored in the TARGET ACCOUNT, including copies of emails sent to and from the account, draft e-mails, the source and destination addresses associated with each email, the date and time at which each e-mail was sent, and the size and length of each email; Any deleted emails, including any deleted information described above;
- I. **Android Device Information:** To include current and previous Device ID, IMEI/MEID, Registered Date/Timestamp, First Check-In Date/Timestamp, Last Check-In Date/Timestamp, Last Check-In IP Address, Google Accounts associated with the device(s), and device hardware information;
- J. **Google Drive:** To include Subscriber Information, Login and Logout IP Addresses and associated date/timestamps, device identifiers for devices accessing Google Drive account. Backups section to see what devices have data backed up to the service as well as the backup of the Device ID identified. To include any documents in My Drive;
- K. **Google Voice:** To include Subscriber Information, Account settings, Account change history, Voicemail Messages, SMS Messages, Greetings and call logs;

- L. **Google Photos:** To include photos and videos from Google Photos and from other Google services, such as Google+, Blogger and Hangouts;
- M. **Google My Activity:** To include Ads, Chrome, Drive, Google Analytics, Google Apps, Google Play Store, Image Search, Maps, Search, Takeout, Video Search and YouTube;
- N. **Google Hangouts:** The communication platform developed by Google which includes messaging, video chat, SMS and VOIP features. To include detailed information in reference to all known outgoing and incoming calls associated with the account, dates and times calls were made, and duration of all calls made or received. This is to include any other pertinent call detail records including special features codes, or any other codes that are maintained in the normal course of business for Google. To include source and destination addresses associated with each communication, the date and time at which communications were sent, and the size and length of each communication. The contents of all stored text messages, voicemails, recorded calls, chat messages associated with the account, for the aforementioned requested time period are also encompassed by this order;
- O. **Deleted Data or Tombstone Data:** In the event any of the requested data has been deleted, please recover any and all data that is still recoverable up to or exceeding a 60-day period, as well as the date/time of deletions;

- P. **Subscriber Information**, including the name and location, supplied by the user at the time of registration, the date the account was created and all of the services of the Target Provider used by the TARGET ACCOUNT;
- Q. Records of user activity for each connection made to or from the Target Accounts, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses, and any telephone, instrument or other unique identifiers collected by the Target Provider and associated with the TARGET ACCOUNT;
- R. All information about each communication sent or received by the TARGET ACCOUNT, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);
- S. All records or other information regarding the identification of the TARGET ACCOUNT, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- T. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, videos and other data files;
- U. All local and long-distance telephone connection records;
- V. All telephone or instrument numbers associated with the TARGET ACCOUNT (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”)); and
- W. All wire and electronic communications held or maintained by the Target Provider at any time in association with telephone communication services, including but not limited to text or SMS messaging and stored audio communications, for the use of or associated with the TARGET ACCOUNT.
- X. Google, LLC is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

- A. All information described above in Section I that constitutes contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2), Distribution of Child Pornography, in the form of the following:
 - (a) Records and information constituting, referencing, or revealing child pornography, as defined in 18 U.S.C. 2256(8);

- (b) Records and information constituting, referencing, or revealing child erotica;
- (c) Records and information referencing or revealing the use or ownership of the gmail account **kreampieqwerty6@gmail.com**;
- (d) Records and information referencing or revealing contact with “Jessica Steins” or jessicasteins99@gmail.com;
- (e) Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved;
- (f) Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved;
- (g) Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved;
- (h) Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography;
- (i) Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.
- (j) For all items described in this section, all metadata, transaction information, storage structure, and other data revealing how the items were created, edited, deleted, viewed, or otherwise interacted with;
- (k) Records and information revealing or referencing information about the device(s) used to access the account;
- (l) Records and information revealing or referencing the identity of the individual who created and used the account;
- (m) Identity of accounts linked by cookies; and

- (n) Records and information revealing the location at the time of the foregoing in Section II of Attachment B.

**PRECAUTIONARY INSTRUCTIONS TO PRESERVE POTENTIAL
PRIVILEGES**

If, during the execution of this warrant, the government discovers materials that are potentially attorney-client privileged or subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue its review until the potentially protected materials have been segregated from other evidence obtained under this warrant. Prior to any further review of the identified potentially protected materials, the Government will notify the Court of the need to establish a court-approved process for review and filtering of the potentially protected materials.

Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, Google LLC shall disclose the responsive data by sending it to the below listed contact.

William M. Hargrove
Task Force Officer
Homeland Security Investigations
HSI RAC Greensboro/Winston Salem
426 Galimore Dairy Rd.
Ste. 100
Greensboro, NC 27409
Cell: 336-215-8764
Email: whargrove@townoflibertync.org

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH
KREAMPIEQWERTY6@GMAIL.COM,
GOOGLE ACCOUNT THAT IS
STORED AT PREMISES
CONTROLLED BY GOOGLE LLC

Case No. 1:24-mj-23

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, William M. Hargrove, a Task Force Officer with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this Affidavit in support of an Application for a Search Warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google, an electronic services provider headquartered at Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched, namely Google / Gmail accounts of **William Ray Hartsell, kreampieqwerty6@gmail.com**, is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an Application for a Search Warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of

Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have personally participated in the investigation described herein and have witnessed some of the facts and circumstances described herein. I have also received information from other federal and local law enforcement and intelligence officials relating to this investigation. The information set forth in this affidavit is based on my own observations and review of documents, or reliable information provided to me by other law enforcement personnel. Because this affidavit is being prepared for the limited purpose of securing the requested search warrants, I have not set forth all facts known to me about this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of 18 U.S.C. § 2252A(a)(2), Distribution of Child Pornography, have been committed by the person or persons who used the Google account **kreampieqwerty6@gmail.com**.

3. Based on my training, experience, and the investigation of the facts summarized in this affidavit, I submit there is probable cause to believe that:

a. **William Ray Hartsell** has committed violations of 18 U.S.C. § 2252A(a)(2), Distribution of Child Pornography, and,

b. there is also Probable Cause to search the information described in Attachment A for evidence of these crimes, further described in Attachment B.

AGENT BACKGROUND

4. I have been designated as a Task Force Officer ("TFO") of the U.S. Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") for approximately 2 years and am currently assigned to the Winston-Salem, North Carolina, Office of the Resident Agent in Charge. I am currently a Detective, employed by the Town of Liberty in North Carolina where I specialized in child exploitation and sexual abuse investigations, which granted my position to be cross-designated and assigned with Homeland Security Investigations for Child Exploitation and Human Trafficking related crimes.

5. While assigned to HSI as a Task Force Officer, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training facilitated by the Internet Crimes Against Children ("ICAC") Task Force held by National White Collar Crimes Center ("NW3C"), National Criminal Justice Training Center ("NCJTC"), North Carolina Justice Academy ("NCJA"), and everyday work relating to conducting these types of investigations. I have received training in child pornography, child exploitation, and sex trafficking and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. My training through NCJTC, NW3C, NCJA and the ICAC Task Force has included undercover chats for child exploitation cases, peer-to-peer file sharing of child pornography, online ads pertaining to enticement of children, and training specific to the Peer-to-Peer file

sharing technology. I am Magnet Certified Computer Forensic Examiner, Cellebrite Cellphone certified forensic examiner (Certified Cellebrite Operator/Certified Cellebrite Physical Analyzer). As part of my duties computer and cellphone phone forensic extractions and review, I have to view, categorize, and determine child pornography as an assigned task for numerous agencies, including my own. Moreover, I am a federal law enforcement task force officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252A (relating to child pornography).

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTES

7. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

a. Title 18, U.S.C. § 2252A(a)(2), prohibits the knowing distribution of (a) any child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including

by computer; or (b) any material that contains child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

DEFINITIONS

1. The following definitions apply to this Affidavit and Attachment B:
 - a. “Child Pornography” includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). Child Sex Abuse Material (“CSAM”) has the same meaning.
 - b. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).
 - c. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. *See* 18 U.S.C. § 2256(2).

f. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).

g. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static,

if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

1. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

m. Google "Gmail" is a free web-based email service developed by Google that allows users to send and receive messages from any computer or device with a web browser.

**SUMMARY CONCERNING PERSONS WHO POSSESS AND COLLECT
CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE
INTERNET RELATES TO THE POSSESSION, RECEIPT AND
DISTRIBUTION OF CHILD PORNOGRAPHY**

8. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with

whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest

in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer-to-Peer networks and other online methods would have gained knowledge of its location through online

communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

9. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their

exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones, and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer (via a USB cable) or connect with a computer via Bluetooth, and transfer data files from one digital device to another. Some "smartphone" users can and do create, communicate, upload, and download child pornography, and communicate with children to coerce them or entice them to produce child pornography or perform sexual acts, by using internet based social media or electronic service providers like Instagram, Snapchat, or Apple (and many others).

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail

service, chat services (i.e., “Instant Messaging”), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, LLC, Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography

with growing frequency, in addition to, or as an alternative to, the use of personal devices.

g. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over a terabyte of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

h. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

i. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at

little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

j. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and on the evidence of known Internet-based communications further described below, there exists a fair probability that evidence regarding the receipt and possession of child pornography will be found in the Gmail account that is the subject of this search warrant, **kreampieqwerty6@gmail.com**, notwithstanding the passage of time.

BACKGROUND CONCERNING GOOGLE ACCOUNT SERVICES

10. In my training and experience, I have learned that the electronic service provider Google LLC provides a variety of services to the public, including electronic mail (“email”) access and free online storage space. Google LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC subscribers and information concerning subscribers and their use of Google LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

11. A Google LLC subscriber can also store files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC, such as Google Drive. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

12. In my training and experience, email providers such as Google LLC generally ask their subscribers to provide certain personal identifying information

when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

13. In my training and experience, Google LLC typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), and other log files that reflect usage of the account. In addition, Google LLC logs and retains the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

14. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the

account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

15. Google LLC's online storage service is known as "Google Drive" and is a file storage and synchronization service. Google Drive allows users to store files remotely on Google servers, synchronize files across devices and share files. It is available on the internet and as a mobile application. Files and folders stored in Google Drive can be shared privately with other users having a Google services account. In essence, Google Drive provides the same features as when a user connects a portable hard drive, such as a USB "thumb drive," to a computer, except the storage space is on Google LLC servers; accessible via the Internet at any time, as long as there is an Internet connection.

16. Google Photos is a photo sharing and storage service developed by Google and is available both on the internet via website and as a mobile application. Google Photos gives users free unlimited storage space for photos and videos, under certain conditions, described below. Google Photos can be configured to sync photos and videos taken with a user's camera to a user's Google Photo account.

17. I know from research and testing that Google Drive and Google Photos are complementary parts of the same Google services account. Photos and videos are stored on a user's Google account's storage space with each account having 15 gigabytes (GB) of free storage, with the option to purchase additional storage space. Files uploaded to a user's Google account via Google Drive count against the 15 GB quota. Files uploaded via Google Photos do NOT count against the account's quota as long as they are uploaded as "High Quality" (Google's term). Google advertises that images/videos uploaded as "High Quality" get an unlimited amount of storage space. Images/videos uploaded in "Original Quality" (Google's term) DO count against the account's quota. The difference between "High Quality" and "Original Quality" has to do with the amount of compression applied to a file, which affects the file's size.

18. I know from knowledge and experience that, by default, the Google Photos mobile application is configured to automatically transfer and store graphics files created on the mobile device to the Google Photos service associated with the Google account. Users also have the option to manually transfer files between Google Photos and Google Drive.

19. Google LLC allows subscribers to obtain Google Drive storage space at the domain name gmail.com, like the account listed in Attachment A. Subscribers obtain an account by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored information concerning subscribers and their use of Google LLC services, such as account access information

and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. In general, files that are transferred to a Google Drive or Google Photos account are stored in the subscriber's storage space on Google LLC servers until the subscriber deletes the data. If the subscriber does not delete files, they can remain on Google LLC servers indefinitely. Even if the subscriber deletes files, they may continue to be available on Google LLC's servers for a certain period of time.

21. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining

the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

22. This Application seeks a Warrant to search all responsive records and information under the control of Google LLC, a provider subject to the jurisdiction of this court, regardless of where Google LLC has chosen to store such information. The government intends to require the disclosure pursuant to the requested Warrant of any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google LLC's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

STATEMENT OF PROBABLE CAUSE

UC Chat Leads to Suspect Distributing Child Pornography

23. On 7/25/2023, I Detective Hargrove, HSI-TFO, began an undercover investigation into child exploitation via the internet. An ad was placed on a site called Doublelist.com. Double list is a known site where offenders will both post and respond to advertisements for the sexual exploitation of minors both in person and via internet communications.

24. An advertisement was placed utilizing the Double list website for the vague information of a mother and a plus 1 (later identified as 9-year-old female). The account was made vague to avoid flagging, which is a common tactic involving those attempting to exploit children as websites have become more sophisticated at attempting to stop criminal activity. Once an ad is placed, emails take place between the parties posting and responding to the ad.

25. Upon receiving an email from the account. KREAMPIEQWERTY6@GMAIL.COM, the subject replied:



Jessica Steins <jessicasteins99@gmail.com>

you have a new message - reply to your ad #35829893040

Doublelist <mailer@mailersp.doublelist.com>
Reply-To: kreampieqwerty6@gmail.com
To: jessicasteins99@gmail.com


Mon, Jul 31, 2023 at 7:25 PM

Please let it be me I need this badly I love lil
Email at kreampieqwerty6@gmail.com snap at needblkpuss
Email backup kreampie6@priest.com

Someone sent you a message on doublelist.com, please reply to this email directly: kreampieqwerty6@gmail.com

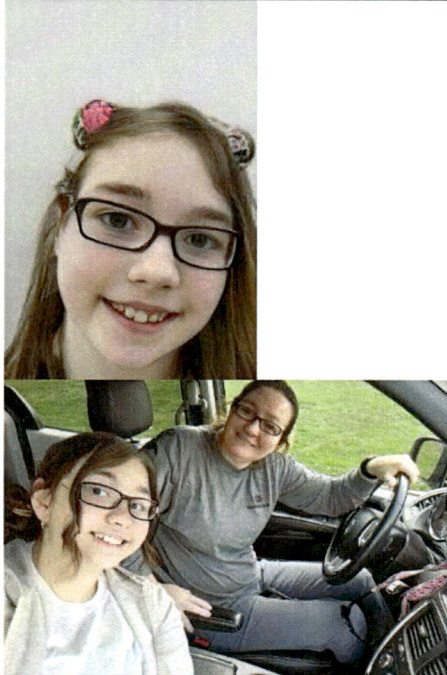
[Quoted text hidden]

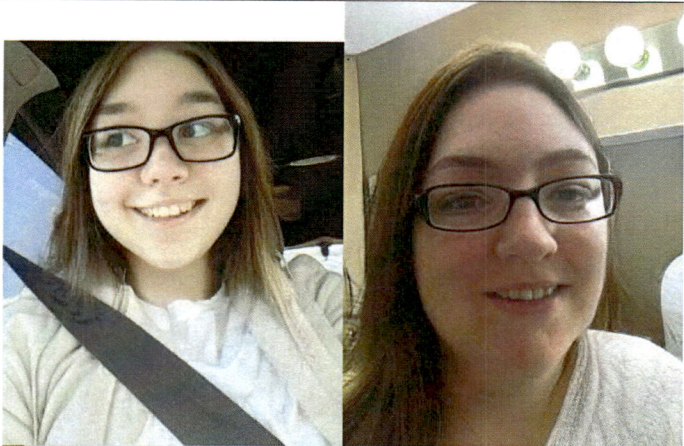

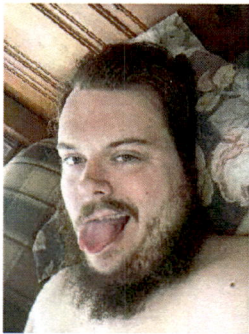
26. The following conversation then occurred via email between Hargrove using the jessicasteins99@gmail.com, “Jessica Steins” account (“Jessica”) and the user of kreampieqwerty6@gmail.com, “Taco Katt,” account later identified as being utilized by Hartsell (“Hartsell”):

From	Email Message	Time/Date
Jessica	What are your limits?	2023-08-02 15:46:58
Hartsell	Virtually none I'm into lil, raw creampie, etc just no blood play as in violence, I do have my red wings lol, age no limits size no limits	2023-08-02 16:35:43
Jessica	Hey that's awesome. Are you willing to help me teach her? This is us 	2023-08-02 16:41:40
Hartsell	Is she willing? Or is this forceful? I'd love details I have sexy pics n vids to prove myself FYI phone about to die on 4 % rn I'll message more when I'm home	2023-08-02 16:46:08
Jessica	Hey I'm 29 and she s 9. No not the cops. The law says if I was I'd have to tell you. We're only here until early Friday morning.	2023-08-02 16:47:03
Jessica	Do you want to text?	2023-08-02 16:47:26
Jessica	Ok that's great. Definitely send me those. Can't wait. Here's my cell 336 396 5918	2023-08-02 16:49:39
Jessica	This is not forcefully at all, she's up for whatever as long as I'm there	2023-08-02 16:50:51
Hartsell	Ok good n can't text wife would find out	2023-08-02 17:38:46

Hartsell	[sends attachment IMG_1363.MOV. Description: This video is approximately one-minute long a depicts a prepubescent minor female, approximately four to eight years old, naked spreading her genitals (focused directly) and sexual in nature, a male voice asks for her to sit on top of him. What appears to be an adult male penis is exposed.]	2023-08-02 17:39:44
Hartsell	[sends attachment <u>trim.CAC1126B-45F6-476A-A4A5-FBF752F66403.MOV</u> . Description: This video is approximately 39 seconds and depicts a pubescent minor female, approximately eleven to fourteen years old, inserting a toothbrush into her anus in a sexual manner.]	2023-08-02 17:40:14
Hartsell	[sends attachment <u>trim.89217F78-E779-4CBA-A430-F3C79E9B5B11.MOV</u> . Description: This video is approximately 42 seconds long and depicts a pubescent female, approximately eleven to fourteen years old, naked except with hand in panties, masturbating.	2023-08-02 17:40:31
Jessica	Oh ok that's cool. What are you down for? We're really open to anything but want it to be a great time. We're from south of Atlanta so don't know anyone there so feel safer here than back at home.	2023-08-02 17:40:39
Hartsell	[sends attachment <u>trim.C47C2772-4304-4E3C-A114-DEDDFF5B5AB0.MOV</u> . Description: This video is approximately 45 seconds long and depicts a pubescent minor female, approximately eleven to fourteen years old, stripping naked, in a sexual manner.]	2023-08-02 17:41:09
Hartsell	Love to raw creampie n eat her out I've been with her age before You said you are house keeping? Can y'all send nudes of y'all?	2023-08-02 17:42:34
Hartsell	[Sends attachment <u>2DF0E0F9-DE4C-4A19-A359-5F7C0F654195.jpeg</u> . Description: This video file depicts a prepubescent minor female, approximately four to eight years old,	2023-08-02 17:43:35

	lying on a bed, naked, sexually posed, with a white fluid that appears to be semen on her chest and face.]	
Jessica	That would be great. I don't know if I should send those of us and get caught.	2023-08-02 17:48:59
Jessica	When could you meet?	2023-08-02 17:51:44
Jessica	You still there?	2023-08-02 18:03:09
Hartsell	Yes and maybe tomorrow or Friday	2023-08-02 18:07:14
Hartsell	Please send them I sent you vids n pics	2023-08-02 18:07:46
Jessica	I'll only be here until early Friday morning. But tomorrow would be good	2023-08-02 18:08:38
Jessica	I'm just nervous	2023-08-02 18:09:32
Hartsell	Ok n please send some	2023-08-02 18:46:41
Jessica	Look if you can't respect us then just forget it we really are looking for a great time but it's up to you. I mean I'll talk to you on phone with both of us or whatever. If you want to come now we're cool with that	2023-08-02 18:58:15
Hartsell	It'll be tomorrow where can you meet	2023-08-02 19:13:35
Jessica	We have a house we're sitting at or can meet you somewhere here. Or if you want to meet somewhere	2023-08-02 19:20:50
Jessica	Do you want to talk on the phone? Or how do you want to do this?	2023-08-02 19:22:46
Jessica	You still there?	2023-08-02 19:59:20
Hartsell	Yea and we can meet in public first then go back to your house	2023-08-02 20:14:43
Hartsell	What time tomorrow n where	2023-08-02 20:14:56
Jessica	1 30? Here at our house. It's on shamrock rd in Asheboro.	2023-08-02 20:15:52
Hartsell	What all did you want to do?	2023-08-02 20:17:34
Hartsell	Address	2023-08-02 20:18:06
Jessica	Anything you want to do, web everything is ok as long as you use condoms.	2023-08-02 20:18:30
Jessica	When u get here in Asheboro I'll give you the address just nervous so you don't come to tonight or something and come hurt us in our sleep	2023-08-02 20:19:46
Jessica	It's really up to I'm not into games ok	2023-08-02 20:22:15
Hartsell	I would never want to hurt y'all cause I want you to come back so we can again and do I have to use condoms I'm married n have to stay clean I'd rather raw creampie y'all	2023-08-02 20:22:45

Hartsell	I'm not for games either I want to fuck y'all both or just her what ever you want	2023-08-02 20:23:19
Jessica	Then we're good just email me tomorrow morning then. I gave you my number to text when you are coming if you don't want to email	2023-08-02 20:25:12
Hartsell	Ok I'll email, so if no nudes can I just see more of y'all? How did you like the vids n pics?	2023-08-02 20:26:14
Jessica	They are good. I showed them to her to believe it's ok to do	2023-08-02 20:32:22
Jessica		2023-08-02 20:33:44

	 	
Hartsell	What she say?	2023-08-02 20:34:11
Hartsell	Ya'll are so beautifull	2023-08-02 20:35:05
Hartsell	Think she can take it?	2023-08-02 20:38:56
	 [Sends two attachments] [the second attachment depicts what appears to be an erect male penis.]	
Jessica	She was amazed.	2023-08-02 20:42:14
Jessica	I think she can definitely take it	2023-08-02 20:54:38
Hartsell	So you ok with no condoms? Raw?	2023-08-02 21:13:17
Hartsell	Are you going to help us fuck? Did too want to fuck too?	2023-08-02 21:24:07

Jessica	Can you bring the condoms. I don't have any and I'll join or just watch but now I'm really excited	2023-08-02 21:49:18
Jessica	Look forward to seeing you	2023-08-02 22:01:04
Hartsell	I really don't wanna use them but ok	2023-08-02 22:27:52
Jessica	Hey are you at least clean, bring them and we can discuss it	2023-08-02 23:10:30
Hartsell	Yes dddf	2023-08-03 00:11:52

27. The conversation continues and the two discuss meeting up. Ultimately, Hartsell does not show up. He indicates his wife was in the emergency room and he had no service.

28. On August 2, 2023, a search of the North Carolina Department of Adult Corrections ("NCDAC") was performed, and a matching suspect named William Ray Hartsell of Charlotte, NC was located. His picture was confirmed through his NC Probation Officer Leftwich as the same person in the picture sent via email at the same time as the picture of an adult male penis.

29. I confirmed with the Mecklenburg County Sheriff's Office that Hartsell was on the Sex Offender Registry, and was provided a report of his previous solicitation of child by computer and appear report. Hartsell had previously solicited an undercover detective of Haywood County NC, posing as a 13-year-old female for sexual activity. NCDAC Probation confirmed his probation status and his residence location of 5317 Allen Rd. E. Charlotte, NC 28269.

30. Probation also confirmed Hartsell has a Dodge Magnum, Black in color, that he drives daily and it now belonged to him and was from a deceased relative.

31. On August 4, 2023, I applied for a search warrant of Hartsell's residence, vehicles, person, and electronic devices. North Carolina Superior Court Judge Taylor Brown found probable cause and issued the search warrant.

32. On August 4, 2023 Charlotte Special Agent ("SA") David Catlano, HSI TFO Rodney Smith, two Charlotte Mecklenburg Police Officers, and I went to Hartsell's Address in Charlotte with arrest warrants for his person and a search warrant. Hartsell met with us and advised he did not want to talk and was then advised of the arrest warrant and search warrant. Hartsell was secured and a sweep of the house was conducted. Hartsell's mother, wife, and infant daughter were at the residence.

33. A search of the residence and vehicles resulted in computers, cellular phones, USB drives, and other electronic devices being seized.

34. Hartsell was taken to a Charlotte Mecklenburg Substation to be interviewed by myself and TFO R. Smith.

35. Hartsell was given *Miranda* Warnings and waived, agreeing to speak with us. Hartsell advised that he felt someone was setting him up but could not think of whom would want to do this to him. Hartsell confirmed that he was the one in fact communicating and arrested before in Haywood County. Hartsell confirmed that is why he was on the sex offender registry. Hartsell even confirmed that he had previously possessed and viewed CSAM, however he had not done that since he was last arrested. Hartsell advised that one of the computers we seized from inside the

residence was old but may contain old CSAM. Hartsell claimed though he was no longer looking at or accessing CSAM.

36. HARTSELL advised he needed food. I took him in my vehicle to go to BOJANGLES to get food and drink. We then headed back towards Randolph County.

37. Hartsell was then placed into the Randolph County Jail and received a \$300,000 secured bond.

38. A download of Hartsell's iPhone revealed that he had searched the UC email (Jessicasteins99@gmail.com) during the operation. Additionally he searched for Shamrock Rd. Asheboro, NC during the operation as was given to the suspect in an email. The pictures he sent of himself to the UC account were also located on the device. All-in-all, there is probable cause to believe that HARTSELL'S Google account contains evidence of distribution of child pornography in violation of federal law.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

40. Based on the foregoing, there is probable cause to believe that the federal criminal statute cited herein has been violated, and that **William Ray Hartsell** has committed the offense. Furthermore, there is probable cause to search the information described in Attachment A for evidence of these crimes, further described in Attachment B. I therefore respectfully request that this Court issue the proposed search warrant.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google LLC. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

/S/ William M Hargrove

William M. Hargrove
Task Force Officer
Homeland Security Investigations

On this 18th day of July 2024, William M. Hargrove appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit.



L. PATRICK AULD
UNITED STATES MAGISTRATE JUDGE